



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,815	10/31/2001	Richard Paul Tarquini	10016862-1	4734

7590 09/07/2005

HEWLETT-PACKARD COMPANY  
Intellectual Property Administration  
P.O. Box 272400  
Fort Collins, CO 80527-2400

EXAMINER
----------

ALOMARI, FIRAS B

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 09/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

10/003,815

Applicant(s)

TARQUINI ET AL.

Examiner

Firas Alomari

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 13 June 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-22 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-22 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

## DETAILED ACTION

### ***Response to Arguments***

1. Applicant's arguments filed 06/24/2005 have been considered but are moot in view of the new ground(s) of rejection.

### ***Claim Rejections - 35 USC § 103***

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-21 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaidya US (6,279,113) in view of Shanklin et al. US(6,578,147).

As per claim 1, 7, 14 and 19: Vaidya discloses a method for detecting an intrusion at node of a network comprising:

Reading a first packet received by the node; ( Col 6, lines 57-59 and item 58 of FIG. 3)

Determining a first signature of the first packet; ( Col 7, Lines 24-30)

Comparing the first signature with a signature file comprising a first machine-readable logic representative of a first packet signature; ( Col 7, Lines 32-36)

Vaidya doesn't explicitly disclose *reading the response packet of the first packet, extracting the signature of the second packet, comparing the signature with the signatures file*. However Shanklin et al. discloses a system for detecting unauthorized signatures from or to a local network where the intrusion sensors analyze inbound and outbound traffic (Col 3, 30-41 and Col 3, Lines 4-7) where he uses the intrusion detection for inbound and outbound traffic. Therefore it would be obvious to one ordinary skilled in the art at the time invention was made to modify Vaidya system with the teaching of Shanklin to include a step for inspecting outgoing response packets and extracting the signature and comparing the signature with the signatures file. One would be motivated to do so in order to enable the system to inspect application level sessions and identify applications that misuses network resources and to enable the system to provide an additional level of security by providing more accurate signature analysis through examining incoming and outgoing packets.

As per claims 2 and 8: Vaidya discloses the method of claim 1, further comprising executing a directive associated with the first machine readable logic upon determining the first signature corresponds with the first machine readable logic. (Col 6, Lines 17-26 and Col 7, Lines 43-45)

As per claims 3 and 9: Vaidya doesn't explicitly disclose the method according to claim 1, further comprising executing a directive associated with the second machine readable logic upon determining the second signature corresponds with the second machine readable logic. however Shanklin et al disclose an intrusion detection system where the IDS sensors examines outgoing packets, sensors forward alerts to a management station which may then alert the system manager or automatically take action(Col 3, lines 55-65). Therefore it would be obvious to one ordinary skilled in the art to modify Vaidya system to include executing a directive for outgoing packets. One would be motivated to do so in order to enable the system to inspect application level sessions and identify applications that misuses network recourses and to enable the system to provide an additional level of security by providing more accurate signature analysis through examining incoming and outgoing packets

As per claim 4,10 and 15: Vaidya doesn't explicitly disclose the method according to claim 3, wherein executing a directive associated with the second machine-readable logic further comprises discarding the second packet. however Shanklin et al. discloses including the appropriate functionality in the sensor to enable it take appropriate action such as terminating the connection (Col 3, lines 55-65 and Col 4, line 54-61). Therefore it would be obvious to one ordinary skilled in the art to modify Vaidya system to include discarding second packets when executing a directive. One would be motivated to do so in order to enable the system to inspect application level sessions and identify applications that misuses network recourses and to enable the system to provide an

Art Unit: 2136

additional level of security by providing more accurate signature analysis through examining incoming and outgoing packets.

As per claim 5 and 11: the method according to claim 4, wherein discarding the second packet further comprises discarding the packet at the network layer of the network stack of the node. The examiner is deeming this to be inherent to the system due to the fact that any processing done at the packet level is done in the network layer of the network stack.

As per claim 6: Vaidya discloses the method according to claim 1, wherein reading a second packet generated by the node in response to reception of the first node further comprises reading a second packet generated by a network stack of an operating system of the node. (*Col 7, Lines 12-24*)

As per claims 12 and 18: Vaidya discloses the computer-readable medium according to claim 7, wherein comparing the first signature with a first instruction set comprising first set of Machine readable logic representative of a packet signature further comprises performing a binary pattern comparison with the first signature and the first set of machine readable logic. (*Col 7, Lines 32-36*)

As per claim 13: Vaidya doesn't explicitly disclose the computer-readable medium according to claim 7, wherein comparing the second signature with the signatures file

further comprises performing a binary pattern comparison with the second signature and the second machine readable logic. however Shanklin et al discloses an intrusion detection system where the IDS sensors examine outgoing packets binary code patterns to detect patterns associated with misused access (*Col 3, Lines 40-49*).

therefore it would be obvious to one ordinary skilled in the art to modify Vaidya system to include binary comparison for outgoing packets. One would be motivated to do so in order to enable the system to inspect application level sessions and identify applications that misuses network recourses and to enable the system to provide an additional level of security by providing more accurate signature analysis through examining incoming and outgoing packets.

As per claim 20: Vaidya discloses the method of claim 19 wherein, wherein the packet is received by the node. (*Col 6, lines 58-65*)

As per claim 21: Vaidya discloses the method of claim 19 wherein, wherein the response packet is received by the node. (*Col 7, lines 24-31*)

As per claim 22: Vaidya doesn't explicitly disclose a step for evaluating if the signature corresponds to a probe packet . However Shanklin et al. discloses a method for detecting probe packets from packets signature( *Col 5, lines 30-55*). Therefore it would been obvious to one ordinary skilled in the art at the time invention was made to modify Vaidya system with the teaching of Shanklin to include an evaluation method for

packets to determine if it belong to a probe packet. One would be motivated to do so in order to enable the system to differentiate between legitimate probe packets and malicious probe packets and to provide protection against different types of attacks.

### ***Response to Arguments***

The applicant's arguments regarding claims 1, 7 & 14 are not persuasive. As Shanklin discloses reading incoming and outgoing data packet in response to communication between two systems (*Col 1, line 63 through Col 2, line 12*) more specifically a session between internal system and an external network entity is monitored (*Col 5, lines 21-39*) it is commonly known in the art that the session communication includes the sent packets and all the consecutive response packets. Furthermore, Shanklin discloses reading a series of packets or a session incoming and outgoing between the computer and the external network through the entry-point networking device, which perform the IDS/IPS function (*Col 2, line 59 through Col 3, line 7 & Col 6, lines 10-24*). Shanklin additionally discloses using composite signatures form each session which include examining each packet's relation ship to adjacent and related packets (*Col 4, lines 54-61*).



***Conclusion***

3. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Firas Alomari whose telephone number is (571) 272-7963. The examiner can normally be reached on M-F from 8:30 am - 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYA Z SHEIKH can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Firas Alomari  
Examiner  
Art Unit 2136

FA

  
Primary Examiner  
AU 2131  
9/2/05